Qual è la differenza fra un virus e un worm?
- Il worm necessita di un programma ospite per replicarsi
- Il virus non è in grado di replicarsi autonomamente
- Il worm necessita di essere eseguito tramite un programma ospite
- **Il virus necessita di essere eseguito tramite un programma ospite**

La diffusione dell'Internet worm del 1988 fu bloccata in breve tempo grazie a:
- **l'esistenza di una rete informale di relazioni fra gli amministratori di sistema Unix**
- l'esistenza di una rete formale di contatti attivabili in caso di incidente (i cosiddetti centri CERT)
- l'efficacia dei programmi antivirus
- il reverse engineering dell'attacco e il corrispondente deployment di opportune regole di firewalling

L'approccio robusto è un principio architetturale secondo cui:
- **Nell'implementazione di un'applicazione di rete è bene essere tolleranti nei confronti dei dati ricevuti e rigorosi nel formattare quelli da spedire.**
- Nell'implementazione di un'applicazione di rete è bene essere rigorosi sia nei confronti dei dati ricevuti che nel formattare quelli da spedire.
- Nell'implementazione di un'applicazione di rete è bene essere tolleranti sia nei confronti dei dati ricevuti che nel formattare quelli da spedire.
- Nell'implementazione di un'applicazione di rete è bene essere rigorosi nei confronti dei dati ricevuti e tolleranti nel formattare quelli da spedire.

Quali livelli della pila protocollare vengono considerati nel modello semplificato TCP/IP?
- Network, Transport, Session, Application
- **Link, Network, Transport, Application**
- Physical, Network, Transport, Application
- Physical, Link, Network, Application

Il principio end-to-end stabilisce che:
- I nodi scartino i dati che provengono da nodi untrusted
- **I nodi elaborino intelligentemente i dati trasmessi dalla rete in maniera neutrale.**
- La rete trasmetta i dati quando i nodi sono in grado di riceverli
- La rete trasmetta i dati, evitando di farlo quando un nodo può causare inefficienze

Il principale problema di sicurezza delle reti locali è dovuto:
- al fatto che fra i nodi non esiste autenticazione
- **al fatto che tutti i nodi condividono un unico mezzo trasmissivo e perciò potenzialmente ricevono tutti i frame, anche quelli non diretti ad un nodo specifico**
- alla possibilità di collegarsi al mezzo trasmissivo in qualsiasi momento
- alla presenza di nodi che, grazie alla condivisione di un unico mezzo trasmissivo, possono alterare il contenuto delle comunicazioni

In che cosa consiste l'attacco denominato MAC flooding?
- Nella cancellazione dell'elenco dinamico di indirizzi MAC che costituiscono un dato collision domain
- Nella saturazione dell'elenco statico di indirizzi MAC che costituiscono un dato collision domain
- Nella cancellazione dell'elenco statico di indirizzi MAC che costituiscono un dato collision domain
- **Nella saturazione dell'elenco dinamico di indirizzi MAC che costituiscono un dato collision domain**

Che differenza c'è fra uno hub e uno switch?
- Uno switch è sostanzialmente un ripetitore di segnale
- **Uno hub è sostanzialmente un ripetitore di segnale**
- Uno hub definisce diversi collision domain
- Uno hub permette di definire confini logici fra i nodi che condividono il medesimo mezzo trasmissivo

Cosa serve la netmask?
- Nelle comunicazioni TCP e UDP, per evitare che un pacchetto raggiunga un nodo di un'altra sottorete
- Nelle comunicazioni TCP o UDP, per distinguere i bit che codificano l'identificatore di un nodo da quelli che identificato la sottorete
- **In una rete IP, per distinguere i bit che codificano l'identificatore di un nodo da quelli che identificato la sottorete**
- In una rete IP, per nascondere la presenza di alcuni nodi al momento inattivi

In che cosa consiste l'attacco ARP poisoning?
- **Nell'alterazione dei dati contenuti nella cache delle associazioni numeri IP numeri MAC**
- Nel mandare una risposta falsa alle richieste ARP di risoluzione di un determinato numero IP
- Nella cancellazione della tabella ARP
- Nell'alterazione del numero MAC di un nodo

Quale di queste affermazioni è falsa?
- **Una comunicazione TCP è identificata dall'indirizzo IP del mittente e da quello del destinatario**
- È possibile avere una connessione TCP nella quale il numero IP del mittente e del destinatario sono uguali
- È possibile avere una connessione TCP nella quale la porta del mittente e del destinatario sono uguali
- Una comunicazione TCP è identificata univocamente da quattro numeri interi

In quale modo è possibile identificare che fra due nodi è in corso una comunicazione che rispetta un determinato protocollo applicativo?
- È sempre possibile perché ogni protocollo è identificato univocamente dalla porta destinazione sulla quale il server è in ascolto
- È impossibile
- È possibile nel caso dei protocolli standardizzati da IANA, perché in questo caso ogni protocollo è identificato univocamente dalla porta destinazione sulla quale il server è in ascolto
- **Non sempre è possibile: in ogni caso occorre esaminare il contenuto del traffico per decidere**

In che cosa consiste il 3-way handshake di TCP?
- **Nella necessità di scambiare tre pacchetti fra client e server prima che la connessione sia considerata stabilita: SYN, SYN-ACK, ACK**
- Nella necessità di scambiare tre pacchetti fra client e server prima che la connessione sia considerata stabilita: SYN, ACK, SYN-ACK
- Nella necessità di scambiare tre pacchetti fra client e server prima che la connessione sia considerata stabilita: ACK, SYN-ACK, SYN
- Nella necessità di scambiare tre pacchetti fra client e server prima che la connessione sia considerata stabilita: SYN-ACK, ACK, SYN

Chi mantiene lo stato di una comunicazione UDP?
- **L'applicazione che utilizza il socket**
- Lo stack protocollare
- La scheda di rete
- Il sistema operativo che fornisce il servizio

La principale difesa in TCP contro l'IP spoofing è:
- il checksum dei pacchetti
- l'autenticazione fra le parti
- **la parziale imprevedibilità del numero di sequenza che contraddistingue i pacchetti SYN**
- la suddivisione dello spazio degli indirizzi in sottoreti

Il TCP fingerprinting:
- consiste nella marcatura crittografica di pacchetti TCP
- permette di riconoscere pacchetti trasmessi piú volte
- permette di identificare i casi di spoofing
- **consiste nell'identificare la specifica implementazione di uno stack TCP per affinare le tecniche di attacco**

Quando lo stato di una porta è closed
- Significa che il firewall filtra gli accessi a quella porta
- Significa che è possibile connettersi solo tramite autenticazione
- Significa che nessuna connessione è possibile
- **Significa che non c'è un socket in ascolto sulla porta accessibile dal numero IP sorgente presente nei pacchetti di SYN**

Secondo il protocollo TCP, ad un SYN diretto verso una porta chiusa
- Si risponde con un SYN-ACK
- Deve essere ignorato
- **Si risponde con un RST**
- Si risponde con un FIN

In cosa differiscono le utility ping e traceroute?
- Sfruttano caratterische differenti del protocollo TCP
- **ping usa un protocollo apposito, mentre traceroute sfrutta i TTL di TCP**
- Sfruttano caratterische differenti del protocollo UDP
- Sfruttano caratterische differenti del protocollo ICMP

In un SYN scan
- **Si risponde con RST al SYN-ACK del server**
- Si manda un FIN al server
- Si mandano pacchetti con flag in combinazioni improprie
- Si mandano pacchhetti con tutti i flag attivati

La tecnica dell'idle scan
- Permette di analizzare le porte aperte di un nodo senza che esso riceva alcun pacchetto proveniente dal nodo scanner
- Permette di attribuire la scansione ad un nodo trusted della rete
- Permette all'attaccante di conoscere i servizi in stato idle
- **Permette di analizzare le porte aperte di un nodo senza che esso riceva alcun pacchetto il cui campo sorgente sia il nodo scanner**

In un Xmas scan
- Si risponde con RST al SYN-ACK del server
- Si manda un FIN al server
- Si mandano pacchetti con flag in combinazioni improprie
- **Si mandano pacchhetti con tutti i flag attivati**

Quale tecnica usa IPsec per impedire gli attacchi replay?
- Vengono crittati i timestamp di invio
- Ogni pacchetto contiene appositi hash crittografici
- **Viene mantenuta una `sliding window' per tracciare i pacchetti già trasmessi**
- La protezione è prevista solo grazie alle caratteristiche di IPv6

Cos'è IPsec?
- Un protocollo per autorità di certificazione
- **Un'estensione del protocollo IP per crittare e scambiare chiavi**
- Un protocollo per gateway
- Un protocollo applicativo per l'autenticazione

Il principale vantaggio di TSL è
- l'autenticazione reciproca di client e server
- la possibilità di avere garanzie di non ripudio
- **la facilità di integrazione con le applicazioni e l'efficienza in presenza di connessioni ripetute**
- l'indipendenza da autorità di certifcazione

In tcpcrypt:
- Si sfrutta un livello di trasporto TSL
- Si usa un 3-way handshake
- **Il carico computazionale è sostenuto per lo piú dai client**
- Le comunicazioni sono obbligatoriamente autenticate

Qual è il compito principale di un firewall?
- **Decidere quale traffico può attraversare i confini di una rete**
- Decidere se il traffico in uscita da una rete è potenzialmente dannoso
- Decidere se il traffico diretto verso una rete è potenzialmente dannoso
- Ridurre il rischio di contaminazione da malware

Quale delle seguenti affermazioni è falsa.
- Esistono firewall che stabiliscono policy ai diversi livelli dello stack TCP/IP
- Un firewall viene installato al confine fra due reti
- **Il traffico che supera il firewall è certamente trusted**
- Perché un firewall sia efficace tutto il traffico fra rete interna ed esterna deve attraversarlo

Che cosa si intende per `packet filter'?
- Un application gateway
- Uno strumento di analisi dei pacchetti
- **Un firewall a livello rete**
- Un circuit gateway

Il termine `deep packet inspection' indica
- **Un firewall stateful che tiene conto del payload dei pacchetti per alcuni protocolli noti**
- Un firewall state-less che tiene traccia delle connessioni verso i nodi piú interni della rete
- Un firewall state-less che conosce un certo numero di protocolli ed è quindi in grado di filtrare in base al contenuto
- Un firewall stateful che tiene conto di tutti i flag

In un firewall `stateful'
- Il filtraggio dei pacchetti tiene conto del contenuto
- Il filtraggio dei pacchetti è particolarmente efficiente
- **Il filtraggio dei pacchetti tiene conto dei pacchetti ricevuti fino a quel momento**
- Il filtraggio dei pacchetti tiene conto dei flag di stato

Cosa si intende per `stateless filtering'
- Una politica di firewalling in cui vengono esaminate tutte le connessioni in una data unità di tempo
- Una politica di firewalling in cui viene esaminato il contenuto di ogni flusso comunicativo
- **Una politica di firewalling in cui viene esaminato ogni pacchetto in isolamento**
- Una politica di firewalling indipendente dalla topologia della rete

Che cosa si intende con il termine `bastion host'?
- **Un nodo particolarmente protetto e capace di difesa prolungata che può essere lasciato al nemico senza danni per la rete interna.**
- Un nodo vulnerabile che può essere lasciato al nemico senza danni per la rete interna che permette di raccogliere dati sugli attacchi.
- Un nodo protetto da firewall in ingresso e in uscita.
- Un nodo protetto da firewall solamente in ingresso.

In un'architettura a `screened subnet'
- Ogni comunicazione, anche interna alla sottorete locale, è sottoposta all'esame del firewall
- **Si usano due firewall per creare una zona di interdizione**
- La rete locale viene divisa in due sottoreti, entrambe difese dal bastion host
- I nodi della rete locale risultano totalmente isolati dalla rete Internet globale

Una politica di firewalling che vieta pacchetti TCP con porta destinazione 22 se provenienti dall'interno e porta sorgente 22 se provenienti dall'interno:
- impedisce si stabiliscano connessioni su di un server interno in ascolto sulla porta 22
- **impedisce si stabiliscano connessioni su di un server esterno in ascolto sulla porta 22**
- impedisce connessioni con tutti i server SSH esterni
- impedisce connessioni con tutti i server SSH interni

Regole di ingress ed egress filtering:
- forniscono una protezione totale rispetto allo spoofing IP
- forniscono una protezione parziale rispetto ai soli attacchi noti
- forniscono una protezione totale rispetto alle falsificazioni dei numeri MAC
- **forniscono una protezione parziale rispetto allo spoofing IP (non proteggono ad esempio da uno spoofing fra nodi della rete locale)**

Il principio del privilegio minimo prescrive che:
- ad ogni ruolo siano concessi tutti e soli i permessi del livello amministrativo minimo
- nel sistema il numero di ruoli amministrativi previsti sia minimo
- a nessun ruolo sia assegnato alcun privilegio amministrativo
- **ad ogni ruolo siano concessi tutti e soli i permessi strettamente necessari alle operazioni assegnategli dal progettista del sistema**

I protocolli firewall-friendly sono quelli:
- **in cui client e server hanno ruoli ben definiti e fissi nel tempo**
- che usano porte comprese fra 1024 e 65535
- che possono essere attivi su i nodi firewall, senza introdurre vulnerabilità nella rete
- che usano porte comprese fra 1 e 1024

FTP è un protocollo firewall-friendly
- **solo nella versione `passiva'**
- quando viene usata la porta 21 per i comandi e la 20 per la trasmissione dei dati
- quando viene usata soltanto la porta 21
- dipende dal firewall

Un proxy
- **opera sia da client che da server**
- impedisce che i nodi della rete interna comunichino con l'esterno
- crea una zona di interdizione fra rete interna e rete esterna
- può essere implementato con un firewall state-less

Un dispositivo NAT:
- **può alterare gli indirizzi IP sorgente e destinazione dei pacchetti che lo attraversano**
- può alterare l'indirizzo IP destinazione dei pacchetti che lo attraversano
- non può alterare gli indirizzi IP sorgente e destinazione dei pacchetti che lo attraversano
- può alterare l'indirizzo IP sorgente dei pacchetti che lo attraversano

Gli HIDS sono:
- **Sistemi che analizzano informazioni relative all'attività locale di un singolo host.**
- Sistemi che utilizzano le informazioni raccolte da analizzatori di traffico di rete.
- Sistemi in grado di riconoscere il malware installato su un singolo host.
- Sistemi in grado di fermare l'attività delle botnet in una rete locale.

Per quanto riguarda la rilevazione di intrusioni per anomalia fra le tecniche di maggior successo va annoverata
- **la verifica di integrità di un sistema per confronto degli MD5**
- la rilevazione del protocollo IRC su macchine MS Windows
- la rilevazione di attacchi su porte ben note
- la rilevazione di virus con stringhe di byte

Un IDS basato su `misuse detection':
- **opera considerando un database di descrizioni di malware noti**
- è in grado di rilevare attacchi imprevisti
- necessita di modelli del comportamento normale degli utenti
- controlla che gli accessi alla rete avvengano secondo le policy aziendali

Un set di regole di un IDS sperimentato su traffico di laboratorio composto da 46 flussi ha dato i seguenti risultati: 20 allarmi corrispondenti ad altrettanti flussi d'attacco, 2 falsi allarmi, 4 attacchi non rilevati. Qual è la specificità dell'IDS?
- 87%
- **91%**
- 83%
- 50%

Cosa rappresenta una curva ROC riferita a un IDS?
- la sensibilità rispetto all'accuratezza
- **la sensibilità rispetto al tasso di falsi positivi**
- la specificità rispetto al tasso di falsi positivi
- l'accuratezza rispetto alla precisione

Un set di regole di un IDS sperimentato su traffico di laboratorio composto da 46 flussi ha dato i seguenti risultati: 20 allarmi corrispondenti ad altrettanti flussi d'attacco, 2 falsi allarmi, 4 attacchi non rilevati. Qual è la sensibilità dell'IDS?
- 50%
- **83%**
- 91%
- 87%

Un set di regole di un IDS sperimentato su traffico di laboratorio composto da 46 flussi ha dato i seguenti risultati: 20 allarmi corrispondenti ad altrettanti flussi d'attacco, 2 falsi allarmi, 4 attacchi non rilevati. Qual è l'accuratezza dell'IDS?
- 83%
- **87%**
- 50%
- 91%

In una determinata rete si stima che si verifichi un attacco ogni 10000 accessi. L'IDS della rete identifica un attacco nel 90% dei casi e genera falsi allarmi nel 5% dei casi. Qual è la probabilità che un allarme corrisponda effettivamente ad un attacco?
- Circa 900 su mille.
- **Circa 2 su mille.**
- Circa 500 su mille.
- Circa 50 su mille.

Il posizionamento di un IDS all'esterno del border router
- può essere utile anche per rilevare attacchi fra i nodi della intranet
- **permette di analizzare informazione completa e non filtrata**
- darà probabilmente luogo a pochissimi allarmi
- è del tutto inutile

Contromisure attivate automaticamente in risposta agli allarmi di un IDS
- sono utili solo nel caso in cui producano un aggiornamento delle regole dei firewall
- **possono peggiorare la gravità degli effetti dell'attacco**
- vanno utilizzate solo nel caso di server che forniscono servizi particolarmente critici
- sono inutili nelle ore diurne

Contromisure attivate automaticamente in risposta agli allarmi di un IDS
- sono inutili nel caso degli IDS misuse based
- sono inutili nel caso degli IDS anomaly based
- sono utili solo nel caso di IDS di rete
- **possono essere sfruttate dall'attaccante come meccanismo d'evasione o di ulteriore attacco**

Il polimorfismo del malware basato su riassegnamento dei registri
- mantiene inalterate le istruzioni macchina, ma varia i dati su cui il malware opera
- funziona solo su macchine RISC
- funziona solo su processori multicore
- **sfrutta il fatto che le istruzioni macchina hanno codice operativi differenti a seconda dei registri coinvolti**

In che cosa consiste la tecnica del `fuzzing'?
- È una tecnica in cui, per identificare vulnerabilità dei firewall, si generano tutte le possibili sequenze di messaggi permessi dai protocolli non filtrati.
- È una tecnica in cui, per identificare vulnerabilità degli IDS, si generano tutte le possibili sequenze di messaggi permessi dai protocolli in uso.
- **È una tecnica in cui, per identificare vulnerabilità dei protocolli, si prova a fornire ai server sequenze di messaggi casuali.**
- È una tecnica in cui, per identificare vulnerabilità dei protocolli, si analizzano tutte le possibili sequenze di messaggi.

Con il termine `honeypot' si intende
- Un sistema particolarmente appetibile per un attaccante
- Un'applicazione malware destinata a indurre gli utenti in operazioni rischiose
- **Un sistema messo in opera con l'unico scopo di essere un potenziale bersaglio di attacchi**
- Un'applicazione malware che apre connessioni in ascolto sulla macchina su cui è installata

I generatori automatici di signature di IDS
- sono inutili nel caso di malware polimorfico
- possono essere usati solo in sistemi con bassi volumi di traffico
- **possono sfruttare il fatto che una parte dei byte d'attacco è necessariamente invariante**
- generano casualmente le signature che poi scartano se causano troppi allarmi

Una botnet di tipo fast-flux
- si diffonde grazie alle vulnerabilità dei servizi IRC
- **nasconde la propria topologia alterando la risoluzione dei nomi simbolici**
- si diffonde grazie alle vulnerabilità dei servizi DNS
- nasconde i messaggi di comando e controllo in conversazioni IRC

Come può essere ridotto il rischio di password guessing?
- Utilizzando password contenenti numeri
- Utilizzando password contenenti segni di interpunzione
- **Aumentando la lunghezza dell'informazione segreta**
- Utilizzando password con caratteri UTF-8

Qual è il vantaggio nel conservare l'hash di una salted password?

- Rende impossibile i dictionary attack
- È un modo di aggiungere cifre alle password, che altrimenti contengono troppi caratteri alfabetici
- È una forma di padding, in modo che tutte le password abbiano la stessa lunghezza
- **Diventa difficile conservare tabelle di hash precalcolati, perché lo spazio delle posiibilità è troppo vasto**

In cosa consiste una Two-Factor Authentication?

- **Si usano due tipi di autenticazione che non possono essere compromessi contemporaneamente**
- Si fa uso di un security token in grado di generare una OTP
- Si usano due password scelte indipendentemente
- Si usa due volte un meccanismo di autenticazione che ha una probabilità di essere compromesso molto piccola

Quale di queste affermazioni sullo schema di Lamport con funzione di hash H è falsa?

- **Non serve alcuna username.**
- Lo schema funziona un numero finito di volte, poi occorre cambiare la password.
- L'autenticando comunica la password cui è stata applicata la funzione di hash un numero di volte n=m-1, dove m è un numero fornito dall'autenticatore.
- L'autenticatore conserva la password cui è stata applicata n volte la funzione di hash.

In un reflection attack:

- **L'attaccante inizia una seconda sessione mentre la prima è ancora in corso**
- L'attaccante è in grado di prevedere il numero casuale generato dall'autenticatore
- L'attaccante è in grado di conoscere la chiave condivisa
- L'attaccante inizia una seconda sessione subito dopo la conclusione della prima

Le autenticazioni con protocolli challenge/response sono vantaggiose perché:

- **Sul canale non passa mai alcunché di segreto**
- Le parti coinvolte nella comunicazione non devono concordare un segreto tramite un differente canale sicuro
- L'autenticazione è sempre reciproca
- Non è possibile indovinare la password tramite tecniche di `forza bruta'

Il protocollo OpenID

- Si basa sull'esistenza di Key Distribution Center trusted
- **Pone problemi di privacy perché permette all'autenticatore di raccogliere informazioni sui servizi utilizzati dall'utente**
- Richiede che gli OpenID provider si accordino sul tipo di credenziali da utilizzare
- Pone problemi di privacy perché rende nota le credenziali di un servizio ad altri servizi indipendenti

Il DHCP è un protocollo utile in particolare quando:

- si ha a che fare con reti la cui topologia è fissa e non si hanno meccanismi di autenticazione basati su numeri MAC
- **si ha a che fare con reti la cui topologia cambia frequentemente e si hanno meccanismi di autenticazione non basati su numeri IP**
- si ha a che fare con reti la cui topologia cambia frequentemente e si hanno meccanismi di autenticazione basati su numeri IP
- si ha a che fare con reti la cui topologia è fissa e si hanno meccanismi di autenticazione basati su numeri MAC

Un attaccante che controlla un rogue DHCP server:
- **può comunicare un gateway di default fasullo in modo da intercettare tutto il traffico generato dai nodi configurati con DHCP**
- può comunicare numeri IP fasulli in modo da falsificare le risoluzioni DNS
- può rendere la rete inutilizzabile con l'address starvation
- può comunicare numeri IP fasulli in modo da intercettare tutto il traffico generato dai nodi configurati con DHCP

Un client DHCP risponde ad una DHCPOFFER di un server con un messaggio broadcast perché:
- in una LAN tutti i messaggi sono broadcast
- non conosce l'IP del server
- **potrebbe esserci piú di un server e il messaggio broadcast permette di fare arrivare a tutti una risposta**
- non conosce il MAC del server

Una rete prevede due DNS. Quali vantaggi ne possono risultare dal punto di vista della sicurezza?
- **Solo uno dei due è esterno, ossia riceve query da utenti esterni per informazioni riguardo host pubblicamente accessibili della rete.**
- Solo uno dei due è esterno, ossia riceve query da utenti esterni per le query ricorsive.
- Solo uno dei due è interno, ossia risolve le query MX riguardo al mail server.
- Solo uno dei due è interno, ossia riceve query da utenti interni per informazioni riguardo host pubblicamente accessibili della rete.

In che modo viene identificata la risposta ad una query DNS?
- **Si tratta di un pacchetto UDP con porta sorgente uguale alla porta destinazione e la genuinità del mittente è controllata tramite il query ID che però spesso è prevedibile**
- Fa parte del medesimo flusso TCP della query, quindi potrebbe provenire da una sorgente falsificata tramite IP spoofing
- Si tratta di un pacchetto UDP che contiene dati firmati con la chiave pubblica del server authoritative, ma non tutti i server sono registrati presso autorità certificatrici affidabili
- Si tratta di un pacchetto UDP con porta sorgente uguale alla porta destinazione usata nella query, quindi l'identificazione del mittente è certa

Un attaccante cerca di avvelenare la cache di un DNS e i suoi messaggi arrivano alla vittima 30ms prima delle risposte authoritative. Supponendo che riesca a mandare 10 messaggi ogni millisecondo:
- può riuscire soltando lanciando un denial of service sul DNS authoritative
- non riuscirà quasi mai nell'intento perché ha una probabilità 300/65536 di indovinare il query ID
- **può riuscire operando anche un proprio DNS authoritative, che permette di ripetere i tentativi**
- non riuscirà quasi mai nell'intento perché ha una probabilità 300/65536 di indovinare la porta UDP

Nel protocollo DNSSEC:
- La chiave pubblica relativa ad una zona viene distribuita dalla zona gerarchicamente inferiore.
- **La chiave pubblica relativa ad una zona viene distribuita dalla zona gerarchicamente superiore.**
- La chiave privata relativa ad una zona viene distribuita dalla zona gerarchicamente inferiore.
- La chiave privata relativa ad una zona viene distribuita dalla zona gerarchicamente superiore.

BGP è un protocollo di routing di tipo path vector:
- significa che l'instradamento avviene considerando la lunghezza dei percorsi possibili
- **significa che l'instradamento avviene consultando tabelle di percorsi possibili**
- significa che l'instradamento avviene considerando il costo dei percorsi possibili
- significa che l'instradamento avviene considerando le politiche di un autonomous system

Gli attacchi esterni a BGP
- **possono essere evitati con una infrastruttura a chiavi asimmetriche ben configurata**
- sono ininfluenti sugli autonomous system non direttamente affetti dall'attacco
- sono intrinseci ai protocolli path vector
- possono essere solo mitigati con regole di firewall di ingress ed egress

L'attacco di prefix hijacking in BGP
- **sfrutta la mancanza di meccanismi di autenticazione nell'ownership di un prefisso**
- sfrutta l'aggregazione di indirizzi con bit in comune
- sfrutta gli errori nelle regole dei firewall
- sfrutta la possibilità di disattivare link instabili

In quale delle modalità 802.11 le stazioni comunicano direttamente senza la mediazione di un'infrastruttura?
- Access point managed
- **Ad-hoc**
- Repeater
- Master

Nelle reti wireless:
- **non si può controllare l'esistenza di collisioni solamente analizzando le caratteristiche del mezzo trasmissivo**
- le collisioni sono ininfluenti, perché si verificano solo tra nodi che non ricevono il segnale dell'altro
- le collisioni sono ininfluenti, perché spesso si verificano tra nodi che non ricevono il segnale dell'altro
- si può controllare l'esistenza di collisioni solamente analizzando le caratteristiche del mezzo trasmissivo

In una rete 802.11 con access point:
- Nelle reti open non è necessaria alcuna associazione, né autenticazione
- è necessario associarsi all'access point conoscendo l'ESSID della rete per poter ricevere dati, mentre per trasmetterne occorre autenticarsi
- per trasmettere e ricevere dati è ncessario autenticarsi, mentre l'associazione serve solo quando sono presenti piú reti
- **è necessario associarsi all'access point conoscendo l'ESSID della rete e autenticarsi per trasmettere o ricevere dati**

Una importante debolezza di WEP consiste nel fatto che
- **I vettori di inizializzazione usati nella produzione dello stream cipher possono essere riutilizzati**
- È basato su RC4 che è facilmente attaccabile
- I vettori di inizializzazione usati nella produzione del block cipher possono essere riutilizzati
- Permette l'uso di chiavi poco sicure

In WEP
- Ogni stazione condivide un insieme di chiavi diverse con l'access point generate con un meccanismo di challenge-response
- Ogni stazione condivide un insieme di chiavi diverse con l'access point distribuite a tempo di configurazione
- **Stazioni e access point condividono una o piú chiavi ditribuite a tempo di configurazione**
- Le stazioni condividono una chiave distribuita a tempo di configurazione

In una rete wireless protetta con WEP
- L'integrità dei frame non è a rischio perché il controllo è un CRC di un messaggio crittato, quindi per falsificarlo occorre conoscere la chiave
- **L'integrità dei frame è a rischio perché il controllo è fatto tramite CRC che protegge solo da errori casuali**
- L'integrità dei frame potrebbe essere a rischio se si trovassero vulnerabilità ai controlli tramite CRC, che al momento però è considerato sicuro
- L'integrità dei frame è a rischio perché non c'è nessun controllo

In WPA per evitare che i vettori di inizializzazione vengano riutilizzati:
- TKIP introduce dei contatori e i frame non in sequenza provocano dissociazione immediata
- TKIP introduce una pairwise master key, chiavi che servono appunto per verificare l'autenticità dei vettori di inizializzazione
- TKIP introduce le pairwise transient key, chiavi che servono appunto per verificare l'autenticità dei vettori di inizializzazione
- **TKIP introduce dei contatori e i frame non in sequenza vengono scartati; inoltre due scarti portano alla dissociazione della stazione**

WPA è considerato piú sicuro di WEP
- **vero, soprattutto perché è difficile riutilizzare i vettori di inizializzazione**
- vero, soprattutto perché la crittografia non usa piú RC4
- falso, perché la maggiore vulnerabilità di entrambi è il controllo di integrità con CRC
- vero, soprattutto perché l'autenticazione avviene attraverso un rete cablata

L'autenticazione WPA2 basata su PSK
- **è vulnerabile ai dictionary attack, intercettando le comunicazioni in fase di autenticazione**
- non è vulnerabile ai dictionary attack, perché le comunicazioni utilizzano AES-128
- è vulnerabile ai dictionary attack, intercettando le comunicazioni in fase di associazione
- è vulnerabile ai dictionary attack, specialmente se si utilizza l'autenticazione 802.1X

Le Privacy-Enhancing Technologies mirano
- solo a controllare in maniera opportuna l'accesso ai dati personali
- **a evitare che vengano accumulati dati personali senza il consenso esplicito del soggetto cui si riferiscono**
- a cancellare i dati personali pericolosi per la privacy delle personalità pubbliche
- ad aggirare le leggi dello Stato
-

La sanitization dei dati consiste
- **nell'eliminare le caratteristiche che li rendono direttamente associabili col soggetto cui si riferiscono**
- nell'aggiungere e togliere in maniera casuale i record di un database
- nel cancellare i dati sensibili
- nel falsificare i dati sensibili

Uno pseudonimo
- non può mai essere collegato all'identità reale
- permette di usare servizi in modo anonimo
- necessita di opportune tecniche crittografiche
- **permette di collegare usi diversi di una risorsa da parte di un soggetto la cui identità rimane nascosta**

L'inosservabilità di un evento E
- **si ha quando non esiste nessun altro evento in grado di aumentare la probabilità a posteriori di E**
- si ha quando esiste un evento F per cui la probabilità a posteriori di E dato F è del 50%
- si ha quando non esiste nessun altro evento in grado di aumentare la probabilità a priori di E
- si ha quando la probabilità a posteriori di E è minore di quella a priori

In una VPN
- **le comunicazioni avvengono tramite un tunnel criptato su di una rete potenzialmente ostile**
- le comunicazioni avvengono su reti pubbliche, ma con un unico amministratore
- si accede alla rete aziendale tramite SSH
- le comunicazioni avvengono su di una rete privata con un unico amministratore

Il port forwarding con SSH
- permette di bypassare qualsiasi firewall aziendale
- è inutile quando viene utilizzato un firewall al perimetro della rete aziendale
- **non assicura la confidenzialità di tutta la comunicazione**
- assicura la confidenzialità di tutta la comunicazione

OpenVPN
- permette di creare VPN solo di livello network utilizzando l'interfaccia TAP
- **permette di creare VPN di livello link e network utilizzando l'interfaccia TUN/TAP**
- permette di creare VPN solo di livello link utilizzando l'interfaccia TUN
- permette di creare VPN solo se non c'è NAT fra i nodi coinvolti

Per difendersi dallo sniffing del traffico web, una buona difesa è
- **HTTPS**
- l'uso di un protocol cleaner
- l'uso di un proxy
- l'onion routing

In un circuito TOR
- ogni nodo conosce il precedente e la destinazione delle celle
- **ogni nodo conosce solo il precedente e il successivo**
- ogni nodo conosce la sorgente delle celle e il nodo successivo
- ogni nodo inoltra in maniera casuale le celle che riceve

Freenet è un sistema che
- **resiste alla censura replicando un file su molti peer, che ignorano di esserne distributori**
- resiste alla censura vietando le ricerche per parole chiave
- espone gli utenti al pericolo di essere identificati come distributori di materiale illegale
- resiste alla censura criptando le comunicazioni fra peer

In una rete TOR
- gli exit node trasmettono solo dati cifrati
- **servono dei directory server trusted**
- si è protetti dalla compromissione di uno qualsiasi degli altri nodi
- si è protetti dalla compromissione di due qualsiasi degli altri nodi

Nei sistemi di condivisione di informazioni peer-to-peer
- l'anonimato è possibile utilizzando un protocol cleaner
- l'anonimato è garantito dall'elevato numero di utenti
- **il tracciamento delle attività è facile, specialmente quando le interazioni avvengono via HTTP**
- il tracciamento delle attività può essere impedito forzando interazioni via HTTPS

Un mix di Chaum
- protegge la confidenzialità dei messaggi solo quando se ne ha a disposizione piú di uno
- evita che il traffico possa essere intercettato
- protegge l'integrità dei messaggi
- **garantisce l'anonimato aumentando, potenzialmente in maniera inaccettabile, la latenza della rete**